

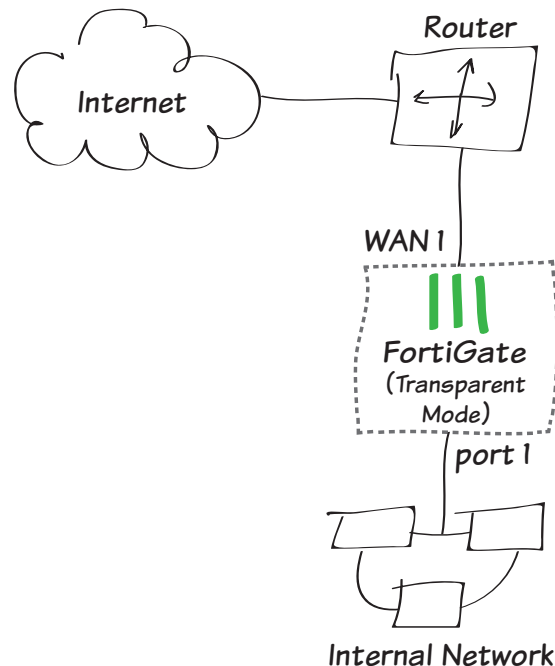
Adding a FortiGate in Transparent mode without changing your existing configuration

In this example, you will learn how to connect and configure a new FortiGate unit in Transparent mode to securely connect a private network to the Internet. In Transparent mode, the FortiGate applies security scanning to traffic without applying routing or network address translation (NAT).



Changing to Transparent mode removes most configuration changes made in NAT/Route mode. To keep your current NAT/Route mode configuration, backup the configuration using the **System Information** widget, found at **System > Dashboard > Status**.

1. Changing the FortiGate's operation mode
2. (Optional) Setting the FortiGate's DNS servers
3. Creating a policy to allow traffic from the internal network to the Internet
4. Connecting the network devices



1. Changing the FortiGate's operation mode

Go to **System > Dashboard > Status** and locate the **System Information** widget.

Beside **Operation Mode**, select **Change**.

System Information	
HA Status	Standalone [Configure]
Host Name	FG100D3G12812324 [Change]
Serial Number	FG100D3G12812324
Operation Mode	NAT [Change]
System Time	Tue Jul 15 09:04:33 2014 (FortiGuard) [Change]
Firmware Version	v5.2.0,build0589 (GA) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	19 day(s) 2 hour(s) 14 min(s)
Virtual Domain	Disabled [Enable]

Set the **Operation Mode** to **Transparent**. Set the **Management IP/Netmask** and **Default Gateway** to connect the FortiGate unit to the internal network.

Operation Mode	Transparent
Management IP/Netmask	172.20.120.122/255.255.255.0
Default Gateway	172.20.120.2

You can now access the GUI by browsing to the Management IP (in the example, you would browse to *http://172.20.120.122*).

2. (Optional) Setting the FortiGate's DNS servers

The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers.

DNS Settings	
<input type="radio"/> Use FortiGuard Servers	<input checked="" type="radio"/> Specify
Primary DNS Server	208.91.123.53
Secondary DNS Server	208.91.123.52
Local Domain Name	

3. Creating a policy to allow traffic from the internal network to the Internet

Go to **Policy & Objects > Policy > IPv4** and create a new policy (if your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6**).

Set the **Incoming Interface** to the available external interface (typically port 1) and the **Outgoing Interface** to the Internet-facing interface (typically WAN1).



It is recommended to avoid using any security profiles until after you have successfully installed the FortiGate unit. After the installation is verified, you can apply any required security profiles.

Incoming Interface	port1	+
Source Address	all	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	any	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	✓ ACCEPT	

Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

Logging Options	
<input checked="" type="checkbox"/> ON	Log Allowed Traffic
<input type="radio"/>	Security Events
<input checked="" type="radio"/>	All Sessions
<input type="checkbox"/>	Capture Packets

4. Connecting the network devices

Go to **System > Dashboard > Status** and locate the **System Resources** widget. Select **Shutdown** to power off the FortiGate unit.

Alternatively, you can enter the following command in the **CLI Console** (also found by going to **System > Dashboard > Status**):

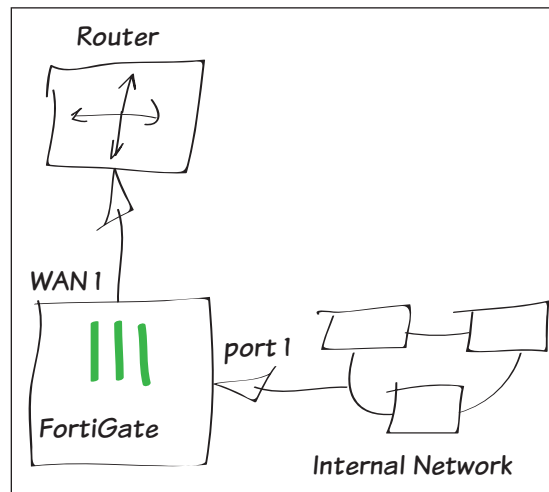
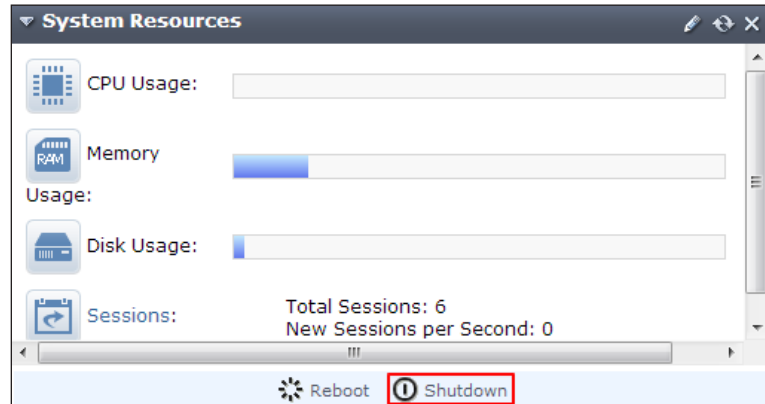
```
execute shutdown
```

Wait until all the lights, except for the power light, on your FortiGate have turned off. If your FortiGate has a power button, use it to turn the unit off. Otherwise, unplug the unit.

You can now connect the FortiGate unit between the internal network and the router.

Connect the wan1 interface to the router internal interface and connect the internal network to the FortiGate internal interface port.

Power on the FortiGate unit.



5. Results

You can now browse the Internet using any computer that connects to the FortiGate's internal interface.

You can view information about the traffic being processed by your FortiGate by going to **System > FortiView > All Sessions** and finding traffic that has port 1 as the **Src Interface** and the Internet-facing interface as the **Dst Interface**.

#	Src Interface	Dst Interface	Dst	Bytes (Sent/Received)
1	wan1	wan1	172.20.120.122	6,567 I
2	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	236 I
3	port1	wan1	s.yimg.com (68.142.250.160:443)	1,026,162 I
4	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	262 I
5	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	291 I
6	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	178 I
7	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	204 I
8	port1	wan1	safebrowsing-cache.google.com (184.150.152.152:443)	10,721 I
9	port1	wan1	BN1WNS1011410.wns.windows.com (157.56.98.65:443)	7,903 I
10	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	211 I
11	port1	wan1	google-public-dns-a.google.com (8.8.8.8:53)	385 I
12	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	226 I
13	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	173 I
14	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	413 I
15	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	204 I
16	port1	wan1	safebrowsing-cache.google.com (184.150.152.178:443)	876,026 I
17	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	184 I
18	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	441 I
19	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	212 I
20	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	204 I

If these two columns are not shown, select Column Settings and move **Src Interface** and **Dst Interface** to the list of fields to be shown.

Column Settings

Available fields:

Application
Device
Dst Address
Dst NAT
Dst NAT Address
Dst NAT Port
Dst Port
Duration
Policy ID
Protocol
Src
Src Address
Src NAT
Src NAT Address
Src NAT Port
Src Port
Timeout
User Name

Show these fields in this order:

Src Interface
Dst Interface
Dst
Bytes